

## Data Protection Policy

Directors Dave Bendell & Chris Foley

Office Manager Debra Wilson

### 1. Introduction

#### 1.1 Background to the General Data Protection Regulation ('GDPR')

The General Data Protection Regulation 2016 replaces the EU Data Protection Directive of 1995 and supersedes the laws of individual Member States that were developed in compliance with the Data Protection Directive 95/46/EC. Its purpose is to protect the "rights and freedoms" of natural persons (i.e. living individuals) and to ensure that personal data is not processed without their knowledge, and, wherever possible, that it is processed with their consent.

#### 1.2 Definitions used by the organisation (drawn from the GDPR)

Material scope (Article 2) – the GDPR applies to the processing of personal data wholly or partly by automated means (i.e. by computer) and to the processing other than by automated means of personal data (i.e. paper records) that form part of a filing system or are intended to form part of a filing system.

Territorial scope (Article 3) – the GDPR will apply to all controllers that are established in the EU (European Union) who process the personal data of data subjects, in the context of that establishment. It will also apply to controllers outside of the EU that process personal data in order to offer goods and services, or monitor the behavior of data subjects who are resident in the EU.

#### 1.3 Article 4 definitions

Establishment – the main establishment of the controller in the EU will be the place in which the controller makes the main decisions as to the purpose and means of its data processing activities. The main establishment of a processor in the EU will be its administrative centre. If a controller is based outside the EU, it will have to appoint a representative in the jurisdiction in which the controller operates to act on behalf of the controller and deal with supervisory authorities.

Personal data – any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special categories of personal data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.



The following outlines the General Data Protection Regulation Policy for Oxford Energy Academy (Compliance From 1/1/2018)

The overarching principle is that.

All data collected and/or stored by Oxford Energy Academy is done so for the sole purposes of Oxford Energy Academy business and an individual's relationship with Oxford Energy Academy.

This will include, but is not limited to, customer communication, internal marketing of events, notification of publications, educational quality standards and CPD.

Individual's personal data will not be shared with a third party without prior written consent.

No member of staff will share any personal data with a third party without the prior consent of the individual. This includes, but is not limited to Name, address, email address and phone details.

All Oxford Energy Academy Staff will sign to consent form for their business email address, phone number and associated business contact details to be circulated for the sole purposes of Oxford Energy Academy business.

All Oxford Energy Academy Staff must agree to allow Oxford Energy Academy to freely use their business contact details but do not agree that they are circulated to external third parties without prior consent on a case by case basis, Staff to avoid using their own personal details for business correspondence.

Oxford Energy Academy Directors and Managers must agree to allow Oxford Energy Academy Staff to freely use their business contact details for the sole purposes of Oxford Energy Academy business but do not agree that they are circulated to external third parties without prior consent on a case by case basis.

#### Data Storage

From May 2018 Oxford Energy Academy will not retain any paper files of personal data, except for financial transactional data.

Oxford Energy Academy will carry out a full IT security audit in collaboration with their specialist IT support contractor and where financial transactional data is retained onsite it will be stored in a locked filing cabinet inside a locked room where access is restricted to the Directors and the Financial administrator.

The data is treated as confidential and is only shared with authorised personal. Authorised personnel include, Directors Office Manager, financial administrator and Accountant. Financial transactional data from previous financial years will be held on site in a secure locked building for 7 years within a secured locked room which only Directors Office Manager, financial administrator and Accountant. have access to.

After their expiry any paper records will be destroyed.

Financial information for online payments are held by Oxford Energy Academy and are all managed by Sage, Oxford Energy Academy hold payment information.



When processing financial information by telephone staff taking the call must not write down or record any of the information given to them except in the designated boxes in the payment terminal. They must not repeat back any card details and if they require clarification they will ask the caller to repeat the details.

The transaction should not be processed on speaker phone, This information should only be inputted by the Directors or financial administrator. This data should not be disclosed under any circumstances.

No PC or workstation shall be left unmanned without a suitable password protected screen saver. All PCs and workstations should be closed and password protected overnight.

All Staff should use only their own login to access PCs and membership databases and not share their login details with others. In order to show compliance to the General Data Protection Regulations all staff will carry out a one-hour online training program so they understand the implications, they will also sign this policy to show they have read and understand their responsibility to personal data.

From May 2018 the Directors and Office Manager will meet quarterly to conduct a GDPR audit to ensure full compliance.

All staff have signed as part of their contract of employment a confidentiality clause. On Joining Oxford Energy Academy each new staff member must be told that the Oxford Energy Academy will not under any circumstances use their data for any other purpose than for processing and marketing Oxford Energy Academy deliverables.

The data will not be circulated to third parties unless staff they give their prior written consent. This is made clear at the beginning of the application process and on every staff review.

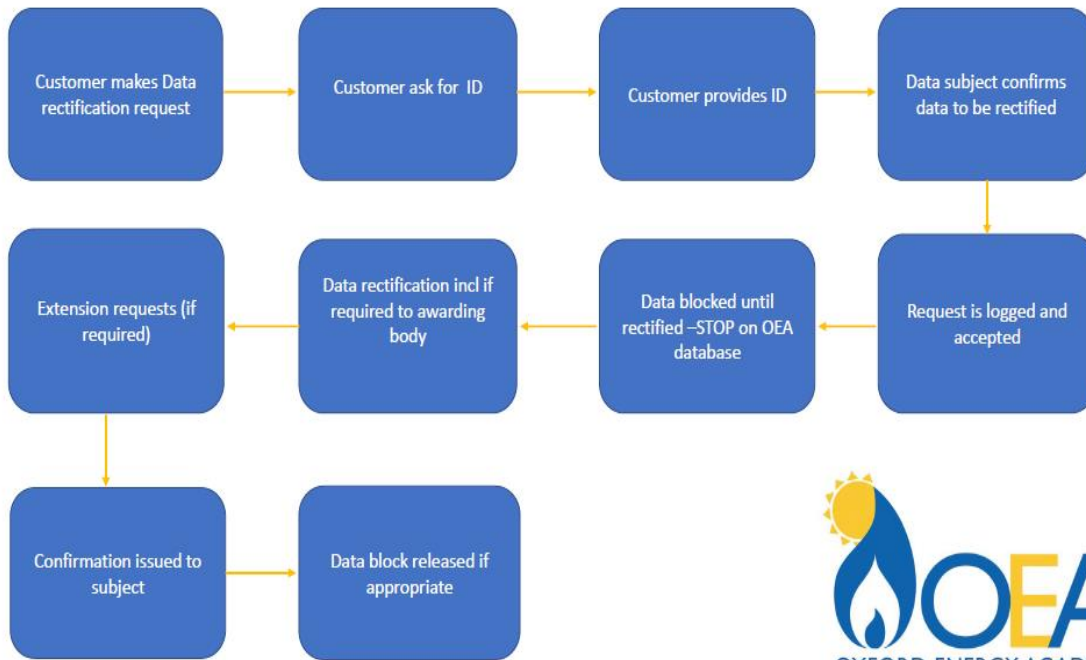
Data Rights. The data held by Oxford Energy Academy can only be as accurate as the information supplied to Oxford Energy Academy. It is the responsibility of the individual to ensure their data is accurate.

Once an individual's relationship with Oxford Energy Academy has become inactive their personal data will be retained electronically for 6 years before deletion as required by awarding bodies. An individual may at any time request the removal of their personal data by Oxford Energy Academy. It should be noted that the removal of all personal data (including email contact details) will result in Oxford Energy Academy no longer being able to carry out the processing of Oxford Energy Academy deliverables. And It may be a requirement by the HSE and Awarding bodies to keep records of training for 6 years • An individual may at any time raise a concern by contacting Oxford Energy Academy Directors.

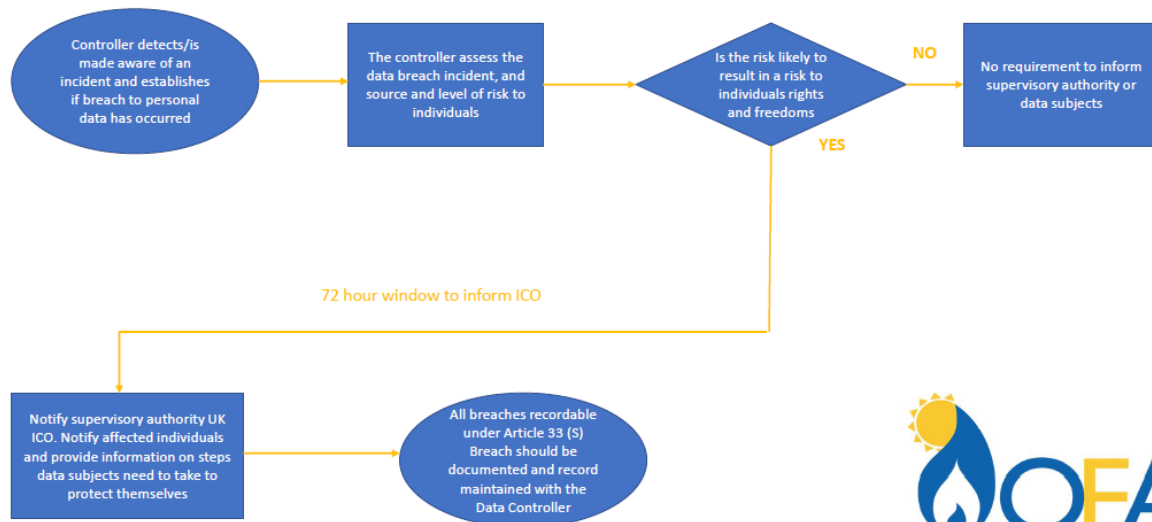
Learner data and documents will be kept until the end of the document retention period as specified by the appropriate body. For the ESF Programme: 2007 to July 2015 ESF programme (until 31st December 2022 at least) and for the August 2015 to 2020 ESF Programme - at least until 31 December 2030 (to be con-confirmed once the Operational Programme is approved)."

Oxford Energy Academy 01993 771155 [info@oxford-energy-academy.co.uk](mailto:info@oxford-energy-academy.co.uk)

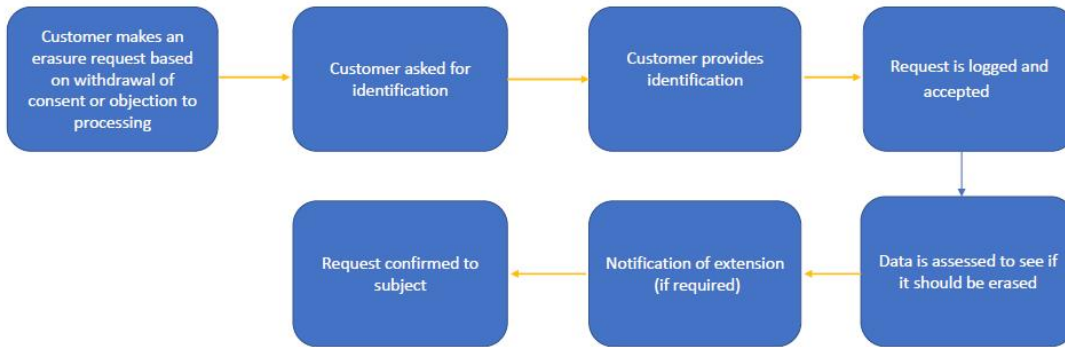
For further details on your rights visit <https://ico.org.uk/for-the-public/>



## Data Rectification Process



## Personal Data Breach Process



## Right to be Forgotten Request-(Customer or Employee)